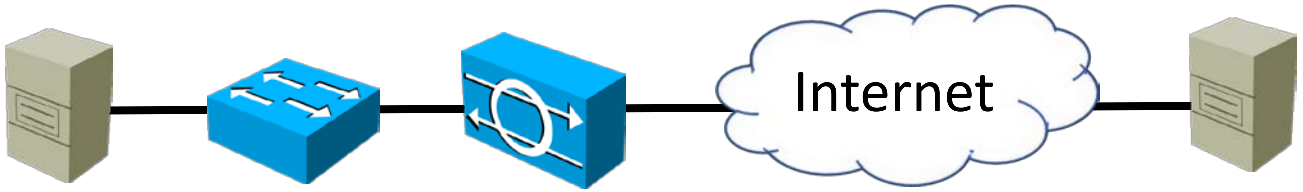
IDS and IPS

- IDS: Intrusion Detection System
- IPS: Intrusion Prevention System
- IDS and IPS use signatures to inspect packets up to layer 7 of the OSI stack, looking for traffic patterns which match known attacks
- They can also use anomaly-based inspection to look for unusual behaviour, such as a host sending more traffic than usual
- They require skilled staff to tune the IPS to their own particular environment and minimize false positives and negatives

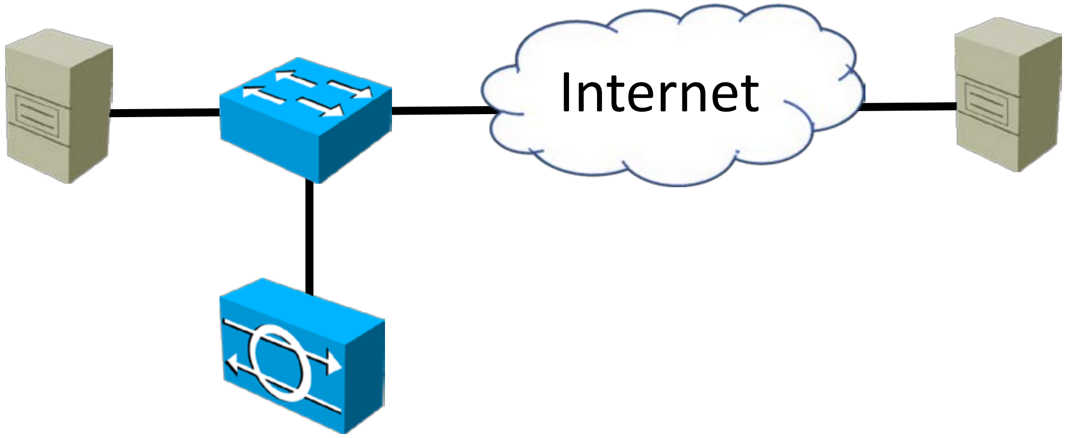
IDS and IPS

- IDS sits alongside the traffic flow and informs security administrators of any potential concerns
- IPS sits inline with the traffic flow and can also block attacks
- (An IDS may also have the capability to tell a firewall to block attacks)

IDS and IPS



IPS



IDS

IPS vs Firewalls

- IPS use **signatures** to inspect packets up to layer 7 of the OSI stack, looking for traffic patterns which match known attacks
- Firewalls block or permit traffic based on **rules** such as destination IP address and port number

IPS vs Firewalls

- Organizations always deploy firewalls on the Internet edge. They may also deploy them at suitable security points inside their internal network
- IPS's are an option which may be deployed in conjunction with a firewall

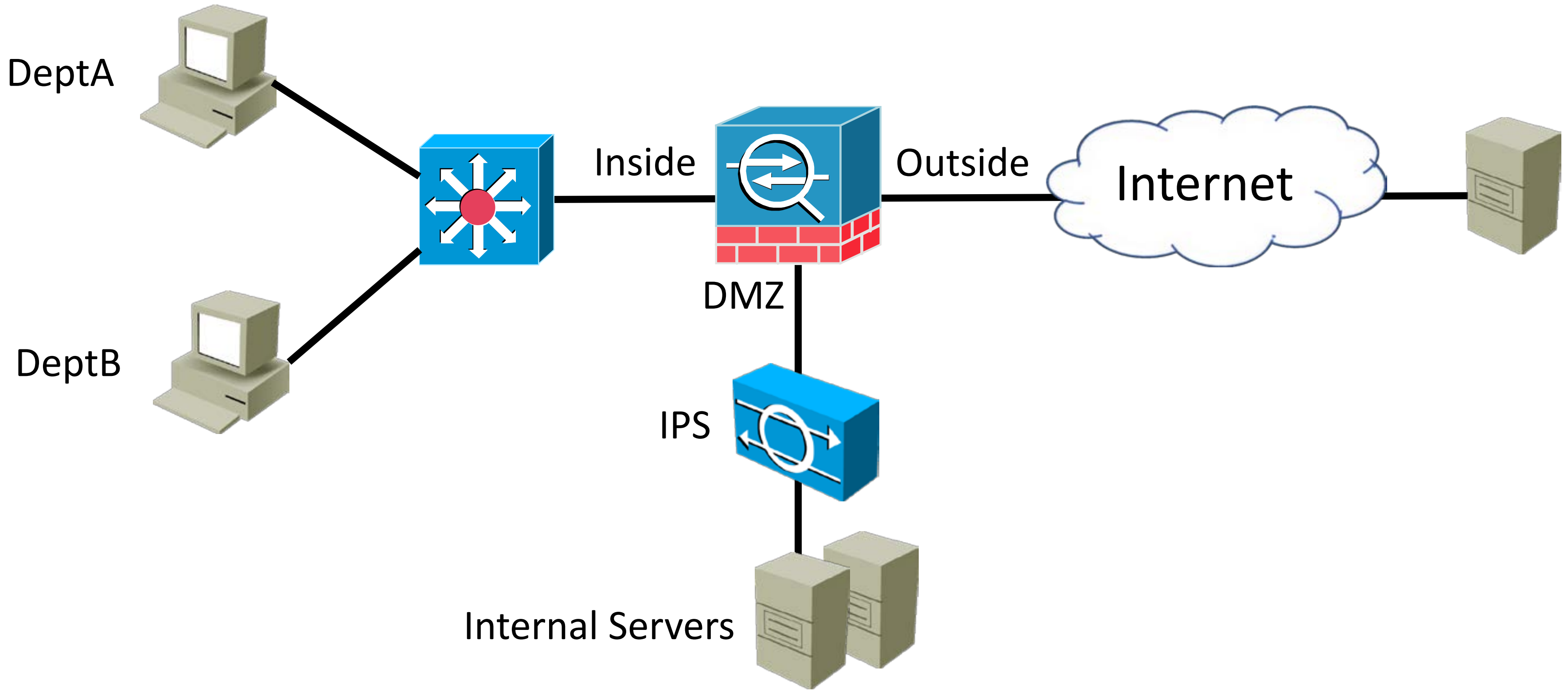
IPS vs Firewalls

- The lines have blurred in recent years between IPS and Firewalls, particularly with the emergence of Next Generation Firewalls
- Modern firewalls often also have IPS capability
- They are also often capable of acting as the endpoint of VPN tunnels

IPS vs Firewalls

- Organisations can deploy an all in one solution, or they may split out the functions to provide better scalability
- Specialised devices may also have more advanced features
- Another option for scalability and higher throughput is clustered devices

Example Firewall and IPS Topology


DeptA
DeptB
Inside
Outside
Internet
DMZ
IPS
Internal Servers